**DD Form 254 Atch 1, IPO Interpretation of 30 Oct 96 NPOESS Security Classification Guide**

Per DD Form 254, Section 13, line c), the NPOESS System Program Director, or designee, shall be responsible for providing any interpretation of the 30 Oct 96 NPOESS Security Classification Guide. The following are the IPO's interpretation of the guidance contained in the 30 Oct 96 NPOESS Security Classification Guidance:

a. Section III, item 1.4 – "Specific impacts to missions supported due to the loss of NPOESS data or capability" applies only to DoD missions, therefore any impacts to the civil sector may be treated as unclassified.

b. Section III, item 1.5 – "Special and/or wartime/contingency mission aspects and related command and control procedures" refers only to information that is of sufficient detail such that, if exploited by a potential hostile entity, that entity could feasibly use it to disrupt or destroy NPOESS operations. This does not apply to general concepts (i.e. data denial) but only to specific processes and implementation details.

c. Section III, item 2.1.1.2 – "Technical details revealing unique propulsion, attitude control, dimensional stability or structural technologies employed" refers only to those technologies that are unique to the United States (i.e. not commercially available) such that, if a rival nation found out about it, that knowledge could cause the US to lose its technical and competitive edge in space.

d. Section III, item 2.2.1 – "Details of specific sensor and payload integration approach for the spacecraft" refers only to information that is unique to the US (i.e. not commercially available) or of enough detail such that, if a rival nation found out about it, that knowledge could cause the US to lose its technical and competitive edge in space. The IPO does not consider integration information presented during reviews to meet this criteria.

e. Section III, item 2.2.2 – "Special Purpose sensors and sensor packages" applies only to sensors that specifically support classified missions as identified by the System Program Director.

f. Section III, item 2.2.4 – "Vulnerability of sensor to environmental and external effects (including radiation, heat, ECM, optical countermeasures, etc.)" refers only to information that is of sufficient detail such that, if exploited by a potential hostile entity, that entity could feasibly use it to disrupt or destroy NPOESS operations.

g. Section III, item 2.2.5 – "Protective measures or capabilities against such effects" refers only to information that is of sufficient detail such that, if exploited by a potential hostile entity, that entity could feasibly use it to disrupt or destroy NPOESS operations. General processes are unclassified if it does not reveal potential weaknesses which could be subject to exploitation.

h. Section III, item 4.1 – "Details of high resolution downlink techniques and data protection measures" refers only to information that is of sufficient detail such that, if exploited by a potential hostile entity, that entity could feasibly use it to disrupt or destroy NPOESS operations.

i. Section III, item 4.2 – "Unique signal processing techniques associated with data processing" does not refer to processing techniques associated with environmental data or satellite state of health data.

j. Section III, item 7.2 – “Protection techniques including radiation hardening, ECM and optical counter-countermeasures” refers only to information that is of sufficient detail such that, if exploited by a potential hostile entity, that entity could feasibly use it to disrupt or destroy NPOESS operations.

k. Section III, item 8.1 – “Specific MMIC technology integration into system sensors” refers only to information that is unique to the US (i.e. not commercially available) or of sufficient detail such that, if exploited by a rival nation, that knowledge could cause the US to lose its technical and competitive edge in space.

l. Section III, item 8.2 – “Focal Plan Array layout and thermal control techniques” refers only to information that is unique to the US (i.e. not commercially available) or of sufficient detail such that, if exploited by a rival nation, that knowledge could cause the US to lose its technical and competitive edge in space.

m. Section III, item 8.3 – “Details of specialized antenna design and construction” refers only to information that is unique to the US (i.e. not commercially available) or of sufficient detail such that, if exploited by a rival nation, that knowledge could cause the US to lose its technical and competitive edge in space.

n. Section III, item 8.3.2 – “Details of specialized manufacturing techniques or unique design features not common to non-sensitive platforms” refers only to information that is unique to the US (i.e. not commercially available) or of sufficient detail such that, if exploited by a rival nation, that knowledge could cause the US to lose its technical and competitive edge in space.

o. Section III, item 8.4 – “Advanced computing and opto-electronic technologies employed in data fusion, processing and distribution operations” refers only to information that is unique to the US (i.e. not commercially available) or of sufficient detail such that, if exploited by a rival nation, that knowledge could cause the US to lose its technical and competitive edge in space.

The IPO is in the process of developing a new NPOESS Security Classification Guide which will incorporate the above IPO interpretation. When validated, it will replace the 30 Oct 96 version and become contractually binding.

**DD Form 254 Atch 2, Attachment to DD Form 254 for Contract No: F04701-02-C-0500**

Communications Security

Reference Block: 10 a

DoD 5220.22-A applies to contractor facilities and operations. Access to **COMSEC** or material or information is restricted to U.S. citizens holding final U.S. Government clearances and is not releasable to personnel holding only a reciprocal clearance. DoD 5522.22A, paragraph 10a(d), personnel must also be briefed on COMSEC for uncontrolled **COMSEC** material. **NACSIM/NACSEM** documents are not considered **COMSEC** controlled material. The Manager of each program will be limited to the minimum necessary, and will be on a strict **need-to-know** basis.

---

**Intelligence Information**

**Reference Block: 10e (1.2)**

If this contract requires access to SCI, the assistant Chief of Staff for Intelligence, USAF, has exclusive security responsibility for all Sensitive Compartmented Information (SCI) classified material released to or developed under this contract this information must be maintained in an SCI facility (SCIF). DIA Manual 50-5, DoD S-5105.21-M-1, and the USAFINTEL 201-1 services provide the necessary guidance for physical, personnel, and information security measures and are part of the security specification for this contract. **Contractor** compliance with these directives is mandatory unless specifically waived. Inquiries pertaining to classification guidance for SCI should be directed to the Contract Monitor (CM).

The following documents with subsequent revision or changes will be used for specific security classification guidance on this contract: USAFINTEL 201-1, 201-4, 201-9, DoD **NISPOM**, and all other security guidance listed in Block 13.

No **Contractor** personnel will be granted access to SCI information/ material under this contract unless they are filling an SCI billet assigned under the contract. The Contract Special Security Officer (CSSO) will coordinate with the Special Project Office Contract Monitor to ensure billets are requested. The names of contractor personnel requiring accessing to SCI will be coordinated through SMC/INS through the Contract Monitor (forms required for a Special Back-ground Investigation (SBI) will be prepared in accordance with the Industrial Security Manual (ISM). Upon receipt of a completed background investigation from Defense Industrial Security Cognizant Office (DISCO), the CSSO will submit a request for SCI eligibility to SMC/INS in accordance with the ISM. Multiple contract employees sponsored by other than SMC/INS must be certified to SMC/INS for placement in a billet.

The **Contractor** will establish and maintain a current access list of SCI personnel on this contract. A copy of the list is provided to the Contract Monitor monthly and when changes occur. The **Contractor** will also advise the Contract Monitor immediately upon the reassignment of personnel to duties not associated with this contract, to include termination.

SCI furnished in support of this contract remains the property of the DoD Department, Agency, or command releasing it. The contractor will maintain an active accountability of all SCI material received, produced, maintained, and disposed of that is in his/her custody, regardless of whether the material is within a contractor or U.S. Government SCI facility. Upon completion

or cancellation of this contract, SCI data must be returned to the custody of SMC/INS unless a follow-on contract specifies that material will be transferred to a subsequent contract. Inventories of SCI material will be conducted in accordance with USAFINTEL 201-1, DIAM 50-5, and DOD S-5105.21-M.

SCI data furnished to or generated by the contractor will require security handling and controls beyond those in the ISM. These supplemental instructions will be furnished and/or made available to the contractor through the Contract Monitor by the User Agency Special Security Office (SMC/INS)

**Release of Information:** SCI with restrictive caveats will be released to contractors only when originator approval has been obtained. The contractor may release such material to any contractor employee working against a billet under this contract and only when a **need-to-know** exists. The contractor may release such material to any Special Security Office personnel assigned to Headquarters Space and Missile Center (HQ SMC), Headquarters Air Force Material Command (HQ AFMC), Headquarters United States Air Force (HQ USAF), or Defense Investigative Agency (DIA) upon demand by such personnel. The **Contractor** will not release this material to other contractors, sub-contractors, or Federal Government agency employees unless the Integrated Program Office Contract Monitor has granted prior written approval. An access certification to a contractor occupied SCIF does not constitute approval to release contractual material to other contractor, subcontractor, or federal government employees; Contract Monitor approval is required. SCI will not be released to non-U.S. citizens (regardless of the level of their security clearance) except with written approval of the originating organization and the Contract Monitor. Contract Monitor approval of a contractor visit certification or permanent certification to another facility will constitute approval to discuss contractual information/material at the facility to be visited.

The contractor will not reproduce any SCI related to this contract without written permission from the Contract Monitor (CM). When such permission is granted, the contractor will control and account for such reproductions in the same manner as the originals.

The NOAA SCIF located in Room 5523, Bldg 3, 1315 East-West Highway, Silver Spring, MD or the SCIF an SMC/IN, Los Angeles AFB, CA, will be used to perform SCI contractual requirements. SCI material released to the contractor under this contract will be stored and worked on only in the aforementioned accredited facility. Any additional SCI contractual work will be accomplished only in an SCI Facility having a current accreditation.

The **Contractor** will comply with the security provisions of DIAM 50-4, 50-5, DOD S-5105.21-M-1, and the SCIF customers **EMSEC** requirements using the attached as a guide.

A CSSO must coordinate with the Contract Monitor and obtain the concurrence of SMC/INS prior to subcontracting any portion of SCI efforts involved in this contract.

The **Contractor** will nominate a CSSO to the NPOESS Security Program Manager who will coordinate this nomination with SMC/INS. In turn, the nomination(s) will be forwarded to HQ AFMC for appointment.

The **Contractor** will not make any type of reference to the level of SCI accesses held, even by unclassified acronyms, in advertising, promotional efforts, or recruitment for employee(s).

The following activity is designated as the User Agency SSO for SCI requirements in accordance with USAFINTEL 201-1, DOD S-5105.21-M-1, AND DIA Manual 50-5.

The User Agency Special Security Officer (SSO) is:

Mr. JOHN Q. PETTIT, GS-13
SMC/INS
(310) 363-0175

SMC/INS (SMC SSO)
180 Skynet Street, Suite 2000
Los Angeles AFB, CA 90245-4690

---

FOR OFFICIAL USE ONLY (FOUO) HANDLING INSTRUCTIONS

Reference Block: 10j

For OFFICIAL USE ONLY (FOUO) Explained:

**FOUO** information is not classified according to Executive Order, but is exempt from disclosure to the public under exemptions 2 through 9 of the **FOIA**. Do not consider or mark any other records **FOUO**. **FOUO** is not authorized as a form of classification to protect national security interests.

Prior FOUO Application:

A **FOUO** marking is not a conclusive basis for withholding a record under the **FOIA**. When such a record is requested, evaluate the information in it to determine if **FOIA** exemptions apply and whether a discretionary release is appropriate.

Time to Mark Records:

Marking records when they are created gives notice of **FOUO** content but does not eliminate the need to review a record requested under the **FOIA**. Examine records with and without markings before release to identify information that needs continued protection and qualifies as exempt from public release.

Distribution Statement:

Information in a technical document that requires a distribution statement according to AFI 61-204 must show that statement. The originator may also apply the **FOUO** marking, as appropriate.

How to Apply FOUO Markings:

Mark an unclassified document containing **FOUO** information **"FOR OFFICAL USE ONLY"** at the bottom, on the outside of the front cover **(if any),** on each page containing **FOUO** information, on the back page, and on the outside of the back cover **(if any).**

In unclassified documents, note that the originator may also mark individual paragraphs that contain **FOUO** information to alert the users and assist in the review process. Mark an individual paragraph in a classified document that contains **FOUO** information, but no classified information, by placing **"(FOUO)"** at the beginning of the paragraph.

Mark an individual page in a classified document that has both **FOUO** and classified information at the top and bottom with the highest security classification of the information on that page.

Mark an individual page in a classified document that has **FOUO** information, but no classified information, **"FOR OFFICIAL USE ONLY"** at the bottom of the page.

If a classified document also contains **FOUO** information, or, if the classified material becomes **FOUO** when declassified, place the following statement on the bottom of the cover or the first page, under the classification marking. If declassified, review the document to make sure material is not **FOUO** and not exempt under the **FOIA** before public release.

Mark other records, such as computer printouts, photographs, films, tape, or slides, **"FOR OFFICIAL USE ONLY"** or **"FOUO"** in a way that ensures the recipient or viewer knows the record contains **FOUO** information.

For **FOUO** material sent outside the DoD to authorized recipients, place an expanded marking to explain its meaning. Do this by typing or stamping the following statement on the document before transfer. This document contains information **EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA**. Exemptions(s) allies (apply). (Further distribution is prohibited without the approval of (enter OPR)).

Procedures for Releasing, Disseminating, and Transmitting FOUO Material:

**FOUO** information may be sent within DoD components and between official of DoD components and authorized DoD contractors, consultants, and grantees to conduct official business for the DoD. Inform recipients of the status of such information, and send the material in a way that prevents unauthorized public disclosure. Make sure documents that transmit **FOUO** material call attention to any **FOUO** attachments. Normally, **FOUO** records may be sent over facsimile equipment. To preclude unauthorized disclosure, consider such factors as attaching special cover sheets, location of sending and receiving machines, and availability of authorized personnel to receive the **FOUO** information. **FOUO** information may be passed to officials in other departments and agencies of the executive and judicial branches to fulfill a government function. Mark the records **"FOR OFFICIAL USE ONLY"** and tell the recipient the information is exempt from public disclosure under the **FOIA** and if special handling instructions apply.

Sending FOUO Information by Unites States Postal Service

Send records containing **FOUO** information in a way that will not disclose their contents. When not mixed with classified information, individuals may send **FOUO** information by First Class Mail or Parcel Post. Bulky shipments, such as distribution of **FOUO** directives or testing materials, that otherwise qualify under postal regulations, may be sent by Fourth-Class Mail.

Electronically Transmitted Messages:

Mark each part of an electronically transmitted message that contains **FOUO** information. Unclassified messages containing **FOUO** information must show the abbreviation **"FOUO"** before the beginning of the text.

Safeguarding FOUO Information:

During Duty Hours. During normal duty hours, place **FOUO** records in and out-of-sight location, if the work area is open to non-government people.

During Non-duty Hours. At the close of business, store **FOUO** records to prevent unauthorized access. File such material with other unclassified records in unlocked files or desks, etc., when the Government or a Government contractor provides normal internal building security during non-duty hours. When there is no such internal security, locked buildings or rooms usually provide adequate

after hour protection. If you desire additional protection, store **FOUO** material in locked containers, such as file cabinets, desks, or bookcases.

The Termination, Disposal, and Unauthorized Disclosure of FOUO:

Terminating **FOUO** Material. The originator of other component authority should remove **FOUO** markings or indicate on the document the markings no longer apply when circumstances show that the information no longer needs protection from public disclosure. When a record is no longer **FOUO**, tell all know holders, to the extent practical. Do not retrieve records in files or storage only for that purpose.

Disposing of **FOUO** Material. Destroy **FOUO** materials by shredding, in any type shredder, to preclude reconstruction.

Unauthorized Disclosure:

The unauthorized disclosure of **FOUO** records is not an unauthorized disclosure of classified information. However, Air Force and DoD contractor personnel have a duty to take reasonable actions to protect **FOUO** records under their control from unauthorized disclosure. Appropriate administrative actions should be taken to fix responsibility for such disclosures and disciplinary action take where appropriate. Unauthorized disclosure of **FOUO** information protected by the Privacy Act (PA) may also result in civil or criminal sanctions against individuals or against the Air Force. Tell the originating organization about an unauthorized disclosure of its records.

Unclassified Controlled Nuclear Information (UCNI):

**UCNI** is sensitive unclassified information subject to special handling as outlined in DoD Directive 5210.83. The likelihood of your company coming in contact with **UCNI** is remote. However, if the situation does arise, employees will protect the information in the same manner as **FOUO** information, contact the company Security Office who, in turn, will obtain guidance from its cognizant Security Office (30 SPS/SPAI).

---

Receive and Generate Classified Material

Reference Block: 11c

Classified material will be handled in accordance with guidance in the **NISPOM** and E.O. 12958

Use of UHF/HF radios, cellular telephones, pages, or other types of resting frequency transmitters is not allowed in a classified processing facilities or areas unless approved by the responsible **EMSEC** Manager.

---

Reference Block: 11d

During the performance of this contract it may be necessary for your company to store classified hardware because of the nature, size, or unique characteristics it may not fit in an approved security container. Your company may have to establish approved closed area(s) in accordance with the National Industrial Security Program Operating Manual (DoD 5220.22-M). The point at which proposed hardware becomes classified shall be provided by the Program Contract Monitor.

---

COMSEC ACCOUNT

Reference Block: 11h

NSA account will be established for and maintained by contractor IAW, the **COMSEC** Annex to the **NISPOM**. (DoD 5220.22A). The Contractor will comply with the additional security requirements and the management of NSA information/material as defined in the Annex.

---

"Other Requirements"

Reference Block: 11L

Program Protection, Systems Security Engineering and Product Security

The contractor shall protect classified national security information, special access and unclassified controlled information, technologies, and critiecal systems as prescribed in Space Systems Protect Guides established under DoD 3500.2; as well as traditional Security Classification Guides applicable to Non-DoD Space Programs.

---

OPSEC

Applicable Block: 11j

The contractor will accomplish the following minimum requirements in support of the User Agency Operations Security (OPSEC) Program.

Document items of critical information applicable to its operations. Items of critical information are those facts, which individually, or in the aggregate, reveal sensitive details about the contractor's security operations, and thus require protections from adversarial collection or exploitation.

Include **OPSEC** as a part of its ongoing security awareness program conducted in accordance with Chapter 3, Section 1, of the National Industrial Security Operating Manual.

Be responsive to the User Agency **OPSEC** Manager on a non-interference basis.

Protect sensitive unclassified information and activities, which could compromise classified information or operations, or degrade the planning and execution of military operations performed by the contractor in support of the mission. Sensitive unclassified information is that information marked **FOR OFFICIAL USE ONLY**, Privacy Act of 1974, **COMPANY PROPRIETARY**, and as identified by the Air Force Program Office and the applicable OPSEC Manager.

---

Additional Security Requirements/Inspections

VI. Reference Block: 14

1. The Assistant Chief of Staff for Intelligence, SUAF, has exclusive security responsibility for all SCI classified material developed or released under this contract. DIAM 50-5, DoDS-5105.21-M and USAF Intel 201 series regulations provide necessary guidance for physical, personnel, and information security measures that are a part of the security requirements for this contract.

2. Access to Intelligence Information. The contractor will require access to other classified intelligence information. The following requirements apply:

a. The **Contractor** is authorized access to classified intelligence information. The most restrictive control marking on the intelligence will ordinarily be: with the approval of the Air Force Chief of Staff, Intelligence (ACS/I), may include intelligence marked: **"DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGNINATOR (ORCON), AND CAUTION PROPRIETARY INFORMATION INVOLVED (PROPIN).**

b. The **Contractor** will comply with the special handling and dissemination requirements specified in the **NISPOM** and the Director of Central Intelligence Directive (DCID) 1/7.

c. The **Contractor** is hereby granted permission to reproduce, extract, distribute (limited to specified Air Force agencies and approved contractor), and destroy or retain the intelligence as required in support of our contract.

d. Intelligence material that, in the judgment of the appropriate Senior Intelligence Officer, should not be handled in this manner and will be so identified in writing at the time of release of the material to the Contractor and procedures for handling and dissemination of that intelligence shall be addressee on an ad hoc basis.